AMENDMENTS TO THE CLAIMS

By this Response, Applicant is amending Claims 2, 5, 17, 27, 29, 37, 48 and 54 and is cancelling Claims 6, 23 and 30 without prejudice or disclaimer. Claims 7–12, 18–20, 22, 24–26, 31–36, 38–40, 49–53 and 55–60 remain as previously presented. New Claims 61–64 have been added.

1. (Canceled)

2. (Currently Amended) A method for identifying a lost or stolen device, the method comprising:

receiving, with a first secure database, input identifying a plurality of devices that have been lost or stolen, wherein each of the plurality of lost or stolen devices is associated with a transmitter;

storing in a second database data identifying at least a portion of the plurality of lost or stolen devices, wherein the second database is in communication with the first secure database;

transmitting with at least one reader an interrogation signal to ~~transmitters of detected devices~~ a transmitter of a detected device;

authenticating the interrogation signal;

receiving identifying information from the ~~transmitters~~ transmitter of the detected device ~~devices~~ with the at least one reader; and

comparing the identifying information of the detected ~~devices~~ device received by the at least one reader with the data stored in the database identifying at least a portion of the plurality of lost or stolen devices so as to locate at least one of the plurality of lost or stolen devices.

3.–4. (Cancelled)

5. (Currently Amended) The method of Claim 2, wherein receiving identifying information from ~~transmitters~~ the transmitter of the detected device ~~devices~~ comprises receiving a signal from a radio frequency identification (RFID) tag associated with [[each]] the detected device.

6. (Cancelled)

7. (Previously Presented) The method of Claim 2, wherein the act of receiving identifying information is performed in a public place.

8. (Previously Presented) The method of Claim 7, wherein the public place comprises an airline terminal.

9. (Previously Presented) The method of Claim 2, wherein the identifying information identifies a laptop computer.

10. (Previously Presented) The method of Claim 2, additionally comprising sending an alarm signal when the information received by the at least one reader corresponds to the data identifying at least a portion of the plurality of lost or stolen devices.

11. (Previously Presented) The method of Claim 10, wherein the act of sending the alarm signal comprises producing an audible tone.

12. (Previously Presented) The method of Claim 10, wherein the act of sending the alarm signal comprises activating an indicator on a display screen.

13.–16. (Cancelled)

17. (Currently Amended) A system for identifying a lost or stolen device, the system comprising:

a transceiver, coupled to a device, the transceiver configured to authenticate an interrogation signal and to transmit identifying information in response to [[an]] the interrogation signal;

a first secure database configured to store data identifying a plurality of lost or stolen devices, the first secure database configured to prevent unauthorized access to the data stored therein; and

a plurality of checkpoints, each checkpoint comprising:

a reader located at the checkpoint and configured to transmit the interrogation signal and to receive the identifying information transmitted by the transceiver, and

a processor configured to compare the identifying information with the data stored in the first secure database, wherein the processor is configured to generate an output signal if the identifying information

matches at least some of the stored data identifying the plurality of lost or stolen devices.

18. (Previously Presented) The system of Claim 17, further comprising an alarm that is configured to receive the output signal from the processor.

19. (Previously Presented) The system of Claim 18, wherein the alarm is configured to produce an audible tone.

20. (Previously Presented) The system of Claim 18, wherein the alarm comprises an indicator on a display screen.

21. (Cancelled)

22. (Previously Presented) The system of Claim 17, wherein the transceiver comprises a radio frequency identification (RFID) tag.

23. (Cancelled)

24. (Previously Presented) The system of Claim 17, wherein at least one of the plurality of checkpoints is located in a public place.

25. (Previously Presented) The system of Claim 24, wherein the public place comprises an airline terminal.

26. (Previously Presented) The system of Claim 17, wherein the device comprises a laptop computer.

27. (Currently Amended) A method for locating a lost or stolen device, the method comprising:

receiving a report of a lost or stolen device having transmitter circuitry attached thereto;

storing data associated with the report of the lost or stolen device into a secure database;

transmitting an interrogation signal with at least one reader;

authenticating the interrogation signal with transmitter circuitry of at least one detected device;

receiving with the at least one reader unique identifying information from the transmitter circuitry of the at least one detected device ~~devices~~, wherein the identifying information is transmitted by the transmitter circuitry of the at least

one detected device ~~devices~~ in response to receiving the interrogation signal; and

comparing the identifying information received by the at least one reader with the data stored in the secure database to locate the lost or stolen device.

28. (Cancelled)

29. (Currently Amended) The method of Claim 27, wherein receiving identifying information from the transmitter circuitry of the at least one detected device ~~devices~~ comprises receiving a signal from a radio frequency identification (RFID) tag attached to each of the at least one detected device.

30. (Cancelled)

31. (Previously Presented) The method of Claim 27, wherein the at least one reader is located in a public place.

32. (Previously Presented) The method of Claim 31, wherein the public place comprises an airline terminal.

33. (Previously Presented) The method of Claim 27, wherein the identifying information identifies a laptop computer.

34. (Previously Presented) The method of Claim 27, additionally comprising sending an alarm signal when the identifying information corresponds to the data associated with the report of the lost or stolen device.

35. (Previously Presented) The method of Claim 34, wherein the act of sending the alarm signal comprises producing an audible tone.

36. (Previously Presented) The method of Claim 34, wherein the act of sending the alarm signal comprises activating an indicator on a display screen.

37. (Currently Amended) An apparatus for identifying a lost or stolen device, the apparatus comprising:

means for receiving a report of a lost or stolen device having transmitter circuitry associated therewith;

secure means for storing data associated with the report of the lost or stolen device;

means for transmitting an interrogation signal and for receiving identifying information transmitted by transmitter circuitry of detected devices in response to receiving and authenticating the interrogation signal; and

means for comparing the identifying information with the data associated with the report of the lost or stolen device to locate the lost or stolen device.

38. (Previously Presented) The apparatus of Claim 37, further comprising means for sending an alarm signal when the identifying information corresponds to at least a portion of the data associated with the report of the lost or stolen device.

39. (Previously Presented) The apparatus of Claim 37, wherein the secure means for storing data comprises a secure database.

40. (Previously Presented) The apparatus of Claim 37, wherein the means for transmitting an interrogation signal and for receiving identifying information comprises a radio frequency identification (RFID) reader.

41.–47. (Cancelled)

48. (Currently Amended) A system for identifying a lost or stolen device, the system comprising:

a transmitter, associated with a device, configured to authenticate an interrogation signal and to transmit identification information in response to ~~receiving an~~ authenticating interrogation signal;

a first transceiver configured to transmit the interrogation signal to the transmitter and to receive the identification information from the transmitter when the transmitter is within a first defined distance from the first transceiver;

a first processor having a first secure database configured to store data identifying a plurality of devices that have been reported as lost or stolen; and

a second processor configured to receive the identification information from the first transceiver, the second processor having a second secure database configured to receive at least a portion of the stored data from the first secure database and configured to compare the received portion of the stored data with the identification information received from the first transceiver to locate at least one of the plurality of lost or stolen devices.

49. (Previously Presented) The system of Claim 48, wherein the first defined distance is approximately six feet.

50. (Previously Presented) The system of Claim 48, wherein the first processor is configured to update the data associated with the plurality of lost or stolen devices stored in the first secure database.

51. (Previously Presented) The system of Claim 50, wherein the second processor is configured to periodically update the second secure database with at least a portion of updated data stored in the first secure database.

52. (Previously Presented) The system of Claim 48, wherein the second processor is configured to generate an alarm if the identification information matches at least a portion of the stored data.

53. (Previously Presented) The system of Claim 48, further comprising:

a second transceiver configured to receive the transmitted identification information when the transmitter is within a second defined distance from the second transceiver; and

a third processor configured to receive the identification information from the second transceiver, the third processor having a third database configured to receive at least a portion of the stored data from the first secure database and configured to compare the received portion of the stored data with the identification information received from the second transceiver.

54. (Currently Amended) A method of identifying lost or stolen items, the method comprising:

receiving data identifying items that have been lost or stolen;

transmitting with a transceiver an interrogation signal directly to a radio frequency identification (RFID) device associated with an item;

<u>authenticating the interrogation signal with the RFID device;</u>

receiving with the transceiver information transmitted by the RFID device in response to receiving the interrogation signal;

storing the data identifying the lost or stolen items in a first secure database;

updating a second secure database with at least a portion of the data stored in the first secure database, the second secure database being in communication with the transceiver; and

comparing the information received by the transceiver with the data stored in the second secure database to locate at least one of the lost or stolen items.

55. (Previously Presented) The method of Claim 54, additionally comprising generating an alarm if the information received with the transceiver matches at least a portion of the stored data.

56. (Previously Presented) The method of Claim 54, wherein the RFID device comprises a memory configured to store said information.

57. (Previously Presented) The method of Claim 54, wherein receiving information transmitted by the RFID device comprises receiving encrypted information.

58. (Previously Presented) The system of Claim 17, wherein at least one of the plurality of checkpoints comprises a corridor configured to allow a person in possession of the device to pass therethrough.

59 (Previously Presented) The system of Claim 48, wherein the identification information is encrypted.

60. (Previously Presented) The system of Claim 48, further comprising a corridor configured to allow a person in possession of the device to pass therethrough, wherein the first transceiver is attached to the corridor.

61. (New) The method of Claim 2, wherein said transmitting with at least one reader comprises transmitting the interrogation signal directly to the transmitter of the detected device.

62. (New) The method of Claim 2, wherein said authentication comprises verifying a password received from the at least one reader.

63. (New) The system of Claim 17, wherein the transceiver comprises a processor configured to perform said authentication.

64. (New) The system of Claim 17, wherein the transceiver is further configured to restrict access to the identifying information stored by the transceiver.